Integritas, Inc – STIX® EHR Release 9.0
Application Service Provider Privacy & Security Policies

Access	It is the policy of Integritas, Inc. that the STIX EHR can only be accessed for update, viewing and reporting by Client-designated users for whom user accounts have been established and maintained by an authorized Client Security Administrator. It is the sole responsibility of Client to appoint one or more Security Administrators with the task of safeguarding user codes and passwords. Furthermore, each Client will have access only to it's own STIX EHR database. Each Client will have a unique database that is separate and distinct from the database of any other Client. It is Client's responsibility to ensure that no other entity than Integritas, Inc. has knowledge of the location, or access links of Client's database. No employee or other representative of Integritas, Inc. or Integritas' hosting partner is allowed access to any database content without the express written permission of Client. All data backup services provided by Integritas or Integritas' hosting partner are "blind" services with respect to database content. In case of an emergency in which Client Security Administrator misplaces or "loses" his or her administration user code or password, Integritas ASP Support will provide a new access password, upon receiving written permission from Client's designated contact representative. In addition, Integritas, Inc. and Integritas' hosting partner will each execute a standard HIPAA Business Associate Agreement, whereby Integritas and hosting partner guarantee appropriate guarding of security and privacy of individual records in accordance to the standards of HIPAA.
Authorization	STIX EHR provides the following client-configurable authorization methods: • User role-based authorization to various levels of secured and confidential information, and • User role-based authorization for various levels of program functionality. • The ability to encrypt all reports and other attachments in emails generated by the system, using an Adobe PDF encryption technology; and
Authentication	STIX EHR provides the following authentication controls: • Unique user code with required password authentication for system login, with a password that requires at least 6 characters; • The user is required to change his/her password upon logging into the software for the first time;

	• The user is prevented from logging into the software after three unsuccessful attempts; • Encrypted passwords; • User authentication to access the database, for open systems databases such as the Oracle or SQL-Server version; • Encrypted data files requiring password authentication to be accessed, for the standard, proprietary database version; • Single user sign-on for accessing the database; and • The ability for a user to lock the workstation, requiring a password for program re-entry. • All passwords must contain at least one alphabetic and one numeric character; • Automatic password expiration, based upon system administration policy; • The user may not re-use the same password, if it has been used in the past five changes; • Automatic user account suspension after an administrator-designated number of unsuccessful login attempts; and • Automatic logoff after a (system administrator-designated) time period of inactivity.
Audit	STIX EHR provides the following client-configurable audit controls: • An historical audit of all individually identifiable protected information that will show who added any record, changed any record, deleted any record or imported any record. The extent and longevity of the audit trail will be governed by the system administrator. • All user accesses to the software, including successful and unsuccessful logins, as well as system logouts. • Changes made to user access rights. • An Event Log of all events that take place in the software that have potential relevance to a Security Administrator
Secondary Uses of Data	Integritas, Inc. does not engage in secondary uses of Client data. All use of the STIX EHR ASP database is restricted to the ASP Client.
Data Ownership	All STIX EHR data is owned exclusively and at all times by the client. In the event that Client decides to terminate use of the ASP, Integritas will provide the complete STIX EHR Microsoft SQL Server database to the client, as well as the security access ownership and password that will enable the client full access to all of their data using standard tools that are readily available for purchase on the open market. These will be provided at no charge to the client, provided Client has paid in full all fees that were previously due Integritas for use of the ASP services, pursuant to the ASP Agreement.

	Should Client elect to bring the STIX EHR system and database in house for use on client's own internal network, Integritas will renegotiate an in-house client-server STIX EHR Licensing and Support Agreement for future use of the software. Integritas does not provide data conversion services for transporting data into other database formats, systems or services. Should Client wish to convert to another system, it will be the responsibility of the client to obtain its own IT consulting services for any data conversion tasks. Integritas is under no obligation or provide such services.